United States Department of the Interior

BUREAU OF LAND MANAGEMENT
California State Office
2800 Cottage Way, Suite W1834
Sacramento, California 95825
www.ca.blm.gov

March 15, 2002

In Reply Refer To:
1280 **(P)**
CA-946

EMS Transmission: 3/15/02
Instruction Memorandum **No. CA-2002-039**
Expires: 09/30/03

To: All California Employees

From: State Director

Subject: Compliance Monitoring of Internet Prohibition for Bureau Laptops

As part of the overall efforts to ensure compliance with the court order on the Department of Interior's connection to the Internet, the Bureau has issued procedures to randomly check Bureau laptops. The procedures for these random audits are described in Instruction Memorandum No. NI-2002-027.

The National Information Resource Management Center (NIRMC) will conduct a random sample of all laptops and provide a list of selected laptops to Rob Cervantes, State Chief Information Officer *(CIO)*. The State CIO will then coordinate assessment of the laptops with the affected employees and their respective offices. Employees will be promptly notified, either by voice mail, e-mail or in person, once their laptop is chosen. Random checks will be completed, as quickly as possible, normally within five (5) working days after identification.

Any compliance violation will be reported to the Bureau's CIO and State Director. Your cooperation is critical in ensuring compliance with court-ordered direction and maintaining our re-connection.

Questions may be directed to Rob Cervantes at (916) 978-4541.

Signed
James Wesley Abbott
Associate State Director

Authenticated
Louise Tichy
Records Management

Attachment:
Instruction Memorandum No. NI-2002-027 (6 pp)

UNITED STATES DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT
NATIONAL INFORMATION RESOURCES MANAGEMENT CENTER
DENVER FEDERAL CENTER, BUILDING 40
P.O. BOX 25047
DENVER, COLORADO 80225-0047

In Reply Refer To:
1280 (NI-140) **N**

February 4, 2002

E-MAIL TRANSMISSION 02/12/2002
Instruction Memorandum **No. NI-2002-027**
Expires: 09/30/2003

To: All Washington Office and Field Officials
Attn: State and Center Chief Information Officers

From: Director, National Information Resources Management Center

Subject: Compliance Monitoring of Internet Prohibition for Bureau Laptops

Purpose: This IM initiates a program of monitoring Bureau laptops to ensure compliance with court-ordered direction to remain disconnected from the Internet until authorized to initiate reconnection proceedings.

Time frame: Immediately.

Policy/Action: Effective immediately implement a monitoring program consisting of the following three steps:

1. Each office will enable dial up network logging for all user laptops. Procedures for accomplishing this are provided in Attachment 1-Enabling Dialup Network Logging.

2. NIRMC will provide periodic (initially every two weeks) random samples of laptops from the Lotus Notes database to select laptops to be assessed for compliance. Lists of the laptops selected as part of the random sample will be provided to the affected State and Center CIOs to coordinate assessment with the affected offices under their jurisdiction. The Sampling Plan is provided in Attachment 2-Sampling Plan for Laptop Compliance.

3. Each office with a selected laptop will examine its log to verify compliance with the prohibition against access to the Internet. Any violations will be reported to the State or Center Director and the BLM CIO. Assessment issues are addressed in Attachment 3-Assessment of Compliance.

Budget Impact: Minor but will affect almost all field offices.

Background: Pursuant to a Temporary Restraining Order entered by the U.S. District Court and a subsequent Consent Order, the Department of the Interior is disconnected from the Internet and may not be reconnected to the Internet until authorized. This policy is applicable to information technology systems, including laptops. In order to assure compliance with this policy, a program of compliance monitoring for laptops will be initiated.

If you have questions or concerns regarding this policy, please contact Joe Wright, Chief, Division of IRM Systems Support, at (303) 236-4066.

Signed By:
Scott MacPherson
Director, NIRMC

Authenticated By:
Linda Graham
NI-100 Staff Assistant

3 Attachments
1 - Enabling Dialup Network Logging (1p)
2 - Sampling Strategy for BLM Laptops (2 pp)
3 - Assessment of Compliance (1p)

Directive forwarded to State Director, CA-940, CA-946 ***2/12/02***

Enabling Dialup Network Logging

Dial Up network logging can be monitored on Windows systems by enabling logging on the various operating systems.

In the **Windows NT 4.0** systems you may do this by:

1. Navigate to the *control panel*
2. *Select modems*
3. *Select modem properties*
4. *Select connection*
5. *Select advanced*
6. *Put a check in the box for Record a log file*.
7. A *systemroot\ModemLog_Model.txt* file will be created and appended to each time the modem is dialed.
8. Change the security setting on the *systemroot\ModemLog_Model.txt* file so non-privileged accounts have read and execute rights only.

In **Windows 2000/XP** this may be accomplished by:

1. Navigate to the *control panel*
2. *Select phone and modem options*
3. *Select modems*
4. *Select modem properties*
5. *Select diagnostics*
6. *Place a check in the box for Append to Log.*
7. A *systemroot\ModemLog_Model.txt* file will be created and appended to each time the modem is dialed.
8. Change the security setting on the *systemroot\ModemLog_Model.txt* file so non-privileged accounts have read and execute rights only.

In the **Windows 9X** client this may be accomplished by:

1. Go to the advanced tab for properties of the dialup adapter.
2. Change *Record a log file* to a value of “yes.”
3. A *systemroot\Model Modem.log* file will be created and overwritten each time the modem is dialed.

Sampling Strategy for BLM Laptops

The following outlines a strategy by which approximately two percent of the BLM's registered laptops can be sampled periodically to verify compliance with the Secretary's directives that DOI laptops not be connected to the Internet.

Sampling will be stratified by both state/center (the first two letters of the BLM organization code of the responsible employee), and by whether the laptop DOES or DOES NOT contain Individual Indian Trust Data (IITD). (Laptops for which the database indicates it MAY contain such data are considered to belong to the DOES -category.)

The sample size for each stratum will be computed as two percent of the stratum population, rounded upward in case this number is not an integer. Due to the effects of rounding a number, the overall percentage of Laptops sampled Bureauwide will be slightly more than two percent.

Stratified sampling is a statistically sound method of estimating population parameters, provided that the estimates from each stratum are properly weighted to account for rounding error. The strategy described here has the additional advantage that separate estimates of compliance can be obtained for each state and for laptops that do and do not contain IITD data.

Assuming intra-stratum homogeneity, stratified sampling is also likely to produce a more accurate estimate of Bureauwide compliance rate. This, as well as statistical measures such as confidence interval, cannot accurately be determined until survey data is collected.

We will sample with replacement---a laptop that has been inspected once might be inspected again. This is an incentive for employees to remain in compliance. The great majority of laptops are in the DOES NOT category; at a two percent sampling rate, employees with these laptops are unlikely to be inconvenienced with frequent repeat inspections. On the other hand, the small number of laptops that do contain IITD are likely to be inspected again and again. This seems reasonable, since the Bureau is believed to have an especially high interest in ensuring that these laptops are kept off the Internet.

Here are the details of the proposed sampling algorithm:

1) Query the database to produce a complete list of Property ID’s of laptops in each stratum.

2) In each stratum, compute a sample size by counting the number of Property ID’s, multiplying by two percent, and rounding upward if the result is not an integer.

3) In each stratum, employ the system random number generator to select from the list of Property ID’s a random sublist of the appropriate sample size.

4) For each Property ID selected, query the database again to retrieve user name, office code, and other necessary identifying information.

5) Contact each identified user with a list of the laptop(s) registered to them that have been selected for inspection.

<><><><><><><><><><><><><><><><>
George Heine, PhD
Mathematical Analyst
National IRM Center
US Bureau of Land Management
<><><><><><><><><><><><><><><><><><><><>

Assessment of Compliance

Manual: Manual assessment of compliance for laptops (selected in a random sample) can be accomplished with examination of the file by a systems administrator when the laptop is recalled.

Tivoli: Automated collection of files may be accomplished through Tivoli for those systems that are Tivoli Endpoints on the network. The individual files may then be examined to see if the modems have been used and if the number called is an authorized number to be accessed.

Other Automated: Automated collection of files on systems which are not Tivoli Endpoints will be more challenging. If the system is connected to the network via LAN card, the file maybe copied from the system using the Admin share. If the system is not connected to the network then a system administrator will need to collect the file manually.